UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANNABELLE ZARATZIAN	)	
PLAINTIFF	)	
	)	
V.	)	10-CV-09049 (VB)(PD)
	)	
ADEL RAMSEY ABADIR AND	)	
LARRY M. CARLIN	)	
DEFENDANTS	)	

PLAINTIFF'S RESPONSE TO DEFENDANT ABADIR'S MOTION FOR SUMMARY JUDGMENT AND CLAIMS IN SUPPORT OF PARTIAL SUMMARY JUDGMENT

Plaintiff**,** Annabelle Zaratzian, replies to the motion for summary judgment filed and served by the defendant Adel Ramsey Abadir in this action and shows that this defendant is not entitled to a summary judgment for all of the following reasons. Plaintiff further claims that she is entitled to partial summary judgment on the issues of auto-forwarding as an interception, that Defendant exceeded his claimed authorization to receive only child related e-mail, and that a fiduciary relationship existed between the parties as a matter of law on December 19, 2006.

I. There are Genuine Disputes of Material Fact

In order to obtain summary judgment, the defendant must establish that there is no genuine dispute as to any relevant fact and that he is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). The defendant's showing as to these matters is defective because factual issues relating to consent and knowledge are not generally amenable to resolution through summary judgment. In this case, a factual dispute exists as to the following issues: (a) whether Plaintiff

consented to the auto-forwarding of her e-mail; and, (b) whether Plaintiff was placed on inquiry notice that her e-mail was being intercepted.

A. Plaintiff did not consent to the auto-forwarding of her e-mail.

The consent exception contained in 18 U.S.C. § 2511(2)(c) is an affirmative defense that must be pleaded and proven by the defendant. A plaintiff need not establish the absence of consent in order to state a claim for relief.[1] Consent only applies to the act of interception; authorization to establish an e-mail account does not equate with authorization to intercept e-mail transmitted to that account.[2] A determination whether consent to an interception existed or occurred is a fact-intensive inquiry.

In *United States v. Willoughby*, the Second Circuit held that the Wiretap Act affords a safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent.[3] While "Congress intended the consent requirement to be construed broadly", the statute does not address specific parameters.[4] Thus, "[i]n the Title III milieu as in other settings, consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." [5] Consent under Title III of the Wiretap Act "is not necessarily an all or nothing proposition; it can be limited [to a particular purpose]." [6]

---

1 *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 19 (1st Cir. 2003)
2 *See e.g. United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991)
3 *United States v. Willoughby*, 860 F.2d 15, 19 (2d Cir. 1988), *cert. denied*, 488 U.S. 1033, 109 S. Ct. 846 (1989);
4 *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987)
5 *United States v. Garcia-Rosa*, 876 F.2d 209, 217-18 (1st Cir. 1989)
6 *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983)

Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception. [7] Implied consent is not constructive consent. Rather, implied consent is "consent in fact" which is inferred "from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance." [8] Thus, implied consent --or the absence of it -- may be deduced from "the circumstances prevailing" in a given situation.[9,10]

The circumstances relevant to an implication of consent will vary from case to case, but will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. The ultimate determination must proceed in light of the prophylactic purpose of Title III -- a purpose which suggests that consent should not casually be inferred. [11]

While the parties agree that Defendant offered to establish an e-mail account for Plaintiff, and that Plaintiff accepted the offer, Defendant has not presented any facts that establish the Plaintiff knowingly or impliedly consented to the interception of her e-mail through auto-forwarding as a result of accepting that offer. Defendant has indicated that Plaintiff consented to the forwarding of e-mail related to the activities of the children. Even accepting this as accurate would mean that Defendant did not have consent for his receipt of any other e-mail messages.

Defendant points to his purported statement to Plaintiff that he would be forwarding her e-mail as evidence of notice. Plaintiff not only denies that this occurred but also denies knowing that auto-forwarding even existed as a means of interception prior to June 27, 2010. While

---

7 *United States v. Lanoue*, 71 F.3d 966, 981 (1st Cir.1995)

8 *Amen*, 831 F.2d at 378.

9 *Campiti v. Walonis*, 611 F.2d 387, 393-94 (1st Cir. 1979)

10 *In re Google Inc.*, 2013 WL 5423918 (N.D. Cal. 2013)

11 *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 24 (1st Cir. 2003).

knowledge of the ability of a system to monitor communications alone cannot be considered implied consent, such knowledge would appear to be an element of implied consent. [12,13]

Defendant also presupposes that authorization to establish an e-mail account necessarily equates with permission to access that account. Access and authorization are not synonymous terms under federal computer misuse statutes.[14]

The Second Circuit has adopted an intended function test with respect to determining whether access to a computer is unauthorized for purposes of a related statute, 18 U.S.C. § 1030.[15] Under this test, when a computer user exploits a weakness in a program and uses a function in an unintended way to access a computer, that access is without authorization. This test should be applicable in the instant case; Defendant Abadir was authorized to use a computer to create an e-mail account for Plaintiff but exceeded that authorization when he accessed her e-mail account through a system function, i.e. the Optimum auto-forwarding rule, that Plaintiff did not authorize.

B. Plaintiff did not have inquiry notice that her e-mail was being intercepted.

Defendant Abadir points to two facts to support his defense that the statute of limitations has run with respect to Plaintiff's claims; his November 11, 2007 e-mail to Plaintiff and a 2008 communication between Plaintiff and the parties' fourteen year old daughter. The fact of that these communications occurred is undisputed, however, their significance at the time is a matter in contention.

---

12 *Campiti*, 611 F.2d at 394.

13 *Jandak v. Village of Brookfield*, 520 F. Supp. 820, 824-25 (N.D. Ill. 1981)

14 Orin S. Kerr, *Cybercrime's Scope: Intercepting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L.R. 1596, 1604 (2003)("At a conceptual level, computer misuse can occur in two distinct ways. First, a user can exceed [his] privileges on a computer, either by using a computer that [he] has no authority to use, or by using the computer in a way that [he] is not authorized to use it.').

15 *Morris*, 928 F.2d at 510.

18 U.S.C. §§ 2520(e) and 2707(f) provide: "A civil action under this section may not be commenced later than two years after the date upon which the claimant first has reasonable opportunity to discover the violation."

"[T]he statute bars a suit if the plaintiff had such notice as would lead a reasonable person either to sue or to launch an investigation that would likely uncover the requisite facts." [16] Circumstantial evidence can be enough to alert a plaintiff to the likelihood of unlawful eavesdropping, if the quantum of evidence is sufficient.[17] While there is no need that someone actually "discover" or be aware of the violation, the question is whether the person had a reasonable opportunity to discover the wiretapping.[18]

A collection of vaguely suspicious circumstances is not enough to place a claimant on notice. [19] Where "the defendant took 'some misleading, deceptive or otherwise contrived action' to conceal information material to the plaintiff's claim," the running of the statute of limitations is tolled. [20] Where there has been fraudulent concealment, "the defendant must show that the plaintiff had 'something closer to actual notice than the merest inquiry notice that would be sufficient to set the statute of limitations running in a situation untainted by fraudulent concealment.'"[21]

The November 11, 2007 e-mail, (Plaintiff's Exhibit 10) which Plaintiff later recognized in 2010 as evidencing a violation of the Wiretap Act, gives no clue as to the source of the information. As Plaintiff testified, at the time she received the message from Defendant she

---

16 *Sparshott v. Feld Entertainment, Inc.*, 311 F.3d 425, 429 (D.C. Cir. 2002).
17 *Id*. at 429-431
18 *Id.*
19 *Cohen v. S.A.C. Trading Corp.*, 711 F.3d 353, 362-63 (2d. Cir. 2013)
20 *Schmidt v. Devino*, 206 F. Supp. 2d 301, 306 (D.Conn. 2001)
21 *Sprint Communications Co., L.P. v. F.C.C.*, 76 F.3d 1221, 1226 (D.C.Cir.1996).

thought someone, perhaps a neighbor, was watching her and relating information to Defendant. See Zaratzian Declaration ¶¶ 30 - 32.

With respect to the 2008 communication between Plaintiff and her daughter, its significance also only became apparent after the interception was discovered in 2010. At the time the comment was made to Plaintiff nothing stated revealed its true source, manner of acquisition, or suggested that it might be tied to the November 11, 2007 e-mail. Further, an alternate explanation – Defendant's contacting Mr. Burke's wife – was plausible and in fact occurred; Defendant had contacted Plaintiff's former husband in 2005 when Plaintiff was divorcing Defendant. Zaratzian Declaration ¶¶ 35-37. On its face, nothing about the comment could have sufficiently alerted Plaintiff that unlawful eavesdropping was occurring especially since a prosecution for e-mail interception by auto-forwarding had not yet occurred in the Seventh Circuit. Put otherwise, what would Plaintiff have been looking for?

Notwithstanding, the disparate nature of these two disclosures occurring over the course of one year, Plaintiff did take steps to review her computer system. On May 22, 2009, well within two years of the November 11, 2007 e-mail, Plaintiff had a technician from "Geek Squad" evaluate the computers in the house. Exhibit 12. This evaluation included an upgrade of hardware and software as well as a diagnostic evaluation. Nothing was discovered, however, because the means of interception existed on the Cablevision/Optimum e-mail servers. And Defendant Abadir never disclosed what he had done to the Plaintiff's e-mail account. As noted in Plaintiff's Statement of Undisputed Facts No. 78, 79, 103, the only way that an Optimum user would know that auto-forwarding has been activated would be to inspect the program settings, something that would not be obvious to either a user or a customer service representative.

Inevitably the factual issue of due diligence involves, to some extent at least, the state of mind of the person whose conduct is to be measured against this test and it is simply not feasible to resolve such an issue on a motion for summary judgment. [22] "What a plaintiff knew and when he knew it, in the context of a statute of limitations defense, are questions of fact for the jury." [23]

II. Defendant is Not Entitled to Judgment as a Matter of Law.

Assuming, *arguendo,* that a genuine dispute of material fact does not exist, defendant is not entitled to judgment as a matter of law on the following issues: (a) whether an interception as defined by 18 U.S.C. § 2510(4) occurred; (b) whether the issuance of temporary protective orders and/or the execution of the Marital Separation Agreement constituted a revocation of any consent that may have been earlier given; (c) whether inter-spousal immunity applies; (d) whether a fiduciary relationship existed at the time the parties executed the Marital Separation Agreement; and (e) whether Plaintiff is entitled to injunctive relief.

A. The auto-forwarding of Plaintiff's e-mail constituted a prohibited interception.

Central to a violation of 18 U.S.C. § 2511 is that an electronic communication be intercepted. Section 2510(4) defines intercept as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device."

Consistent with modern telecommunications engineering, the First and Seventh Circuits have recognized that e-mail messages in transient storage incident to transmission may be subject to interception.[24,25]

The First Circuit in *United States v. Councilman* held that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication

---

[22] *Robertson v. Seidman & Seidman*, 609 F.2d 583, 591 (2d Cir. 1979)
[23] *Riddell v. Riddell Wash. Corp.*, 866 F.2d 1480, 1484 (D.C. Cir. 1989)
[24] *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005)*(en banc).*
[25] *United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010).

process thereby recognizing that e-mail messages in transient storage could be intercepted.[26] This conclusion was supported in part by an amicus brief submitted by a number of technical experts who aptly recognized that "storage [of e-mail] occurs only at the endpoint when a message is accessible to the intended recipient." [27]

As noted in the *Councilman* amicus brief, transmission of an e-mail message is akin to sending a conventional letter from New York to Los Angeles. A letter,

> [M]ight travel from one post office to a central sorting station in the East, to another sorting station in the West, to another post office, before being delivered in Los Angeles. Similarly, an email is sent through a series of computers on the network before it reaches its intended addressee. Each of these computers has its own MTA [mail transfer agent] which is responsible for this hop-to-hop forwarding of the messages through the network. Upon receiving an email, each of these computers checks the address of the recipient, and then determines where to send the email next based on its final destination....
>
> Eventually the email arrives at the recipient's MTA [mail transfer agent], which for these purposes is analogous to the hometown post office of the addressee. At this point, the message is like a letter sitting in a hopper at the local post office waiting to be delivered. Though it may be stored as a part of the process of its delivery, it is still in transmission for all practical purposes because it has not yet been made accessible to its intended recipient.
>
> A mail delivery agent ("MDA") then acts as the postal carrier by determining which user should receive the email and placing the message in the user's mailbox. [28]

Graphically, the transmission of e-mail can be represented as follows:[29]

---

[26] *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005)*(en banc).*

[27] *Exhibit* 22. Amicus Brief of Technical Experts at 3, *United States v. Councilman* (No. 03-1383) November 15, 2004.

[28] *Id*. at 4,5

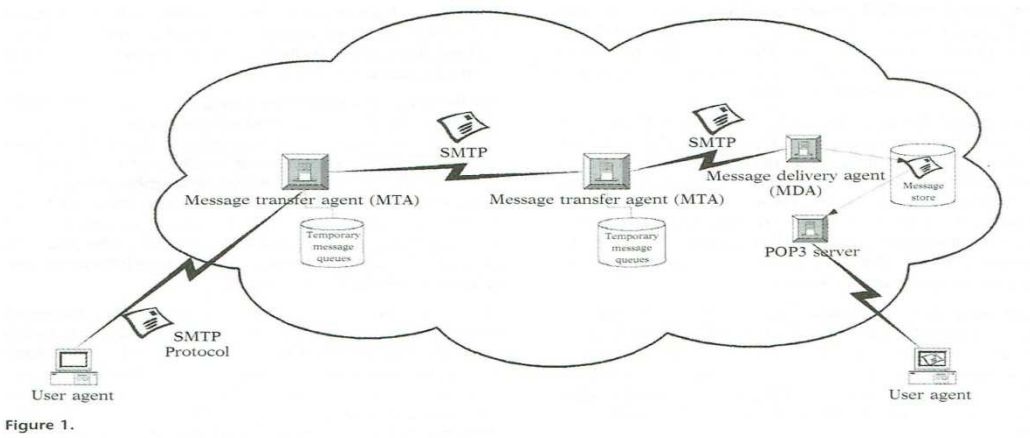

Figure 1.

In *United States v. Szymuszkiewicz*, the Seventh Circuit undertook a detailed examination of how modern e-mail communications are transmitted and received, a process known as "packet switching". The court recognized that "the "interception" of a communication sent in packets must be done by programming a computer to copy the contents it sends along (and reassemble them later)." [30] *Szymuszkiewicz* involved the interception of e-mail through the activation of an e-mail auto-forwarding rule.

Consistent with the technical descriptions in *Councilman* and *Szymuszkiewicz*, Timothy Chase, Director of High Speed Data Security at Cablevision, testified that Optimum e-mail is similarly transmitted.[31]

In order to distinguish a violation of §2510 (Wiretap Act) from a violation of § 2701 (Stored Communications Act), the point at which the e-mail is acquired must be ascertained.[32] Mr. Chase testified that the Optimum auto-forwarding instruction is server based - it is not based

---

[29] Encyclopedia of Computer Science 638 (Anthony Ralston et al, eds. Nature Publishing Group 4th Ed. 2000)

[30] *Szymuszkiewicz*, 622 F.3d at 706.

[31] Plaintiff's Statement of Undisputed Facts Nos. 72 - 75.

[32] *See e.g. Chen v. Romo*, 2013 WL 6814691 (D. Mass, Dec. 20, 2013)

on the client's computer.[33] As such, the forwarding rule is implemented at the mail transfer agent [MTA] level, not at the mail store, or mailbox, level.[34]

Mr. Chase's evaluation of the header information contained in two e-mail messages demonstrates that implementation of the rule occurs at the MTA level. Mr. Chase was asked to compare the e-mail message that Plaintiff received from her accountant, Charles Gomez on June 3, 2009 [Zaratzian 862] with the same message that was forwarded to Defendant Abadir [ABADIR00810]. Review of the message forwarded to Defendant Abadir revealed that when the original message reached MTA23, it was routed to Defendant's e-mail account. Comparison of the two messages revealed that the routing to Defendant occurred at the same moment the original message was routed to Plaintiff.[35] Despite Defendant's contention, the message transmitted to the Defendant was not copied out of the Plaintiff's message store - it was independently transmitted. [36]

Recognition that automatic e-mail re-routing may constitute an interception has also been recognized in dicta by the Eleventh Circuit. As noted in *United States v. Steiger*:

> [T]here is only a narrow window during which an E-mail interception may occur - the seconds or milli-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.[37]

---

[33] Plaintiff's Statement of Undisputed Facts Nos. 70-71.
[34] *Id.* at No. 85
[35] *Id.* at Nos. 86-101.
[36] *Id*. at No. 106.
[37] *United States v. Steiger*, 318 F.3d 1039, 1051 (11th Cir. 2003) (citing Jarrod J. White, *E-Mail at Work.com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997)(*Steiger* involved the anonymous hacking into of the Defendant's computer to download images, e-mail and identifying information stored on his hard-drive. All of the acquired information was obtained while residing on the Defendant's computer.)

A sound technical basis exists for recognizing that an interception pursuant to 18 U.S.C. § 2510(4) may result from the auto-forwarding of e-mail using a server-based rule. Given that the system architecture upon which current e-mail technology rests is not Circuit specific, recognition by this court that the unauthorized automatic re-routing of e-mail violates § 2511 will effectuate a central purpose of the Electronic Communications Privacy Act, namely privacy.

B. The issuance of temporary protective orders and/or the execution of the MSA constituted a revocation of any previously given consent that may have been provided.

Defendant's argument that Plaintiff could not impliedly withdraw her consent to e-mail interception presupposes that Plaintiff knew that her e-mail was being intercepted. Clearly, only once she had notice that her e-mail was being intercepted could such consent be expressly revoked. Until such time as Plaintiff had notice that Defendant was intercepting her e-mail and granted Defendant permission to do so, Defendant had an ongoing affirmative legal obligation to not intercept her e-mail. Post-separation circumstances such as the issuance of temporary protective orders and the obligations imposed upon the Defendant under the MSA only serve to reinforce this obligation.

In the instant case, after Defendant Abadir established Plaintiff's e-mail account using her mother's name as a password, Plaintiff changed the password to "karate", a password she maintained until November 2005. However, Plaintiff could have changed her password one hundred times and the result would have been the same simply because Plaintiff did not know that her e-mail communications were being automatically forwarded to another account

maintained by Defendant. Absent Plaintiff's terminating her account, his account or deactivating the forwarding settings, her e-mail would continue to be routed to his e-mail account.[38]

Plaintiff's situation is fundamentally different from the circumstances presented in the cases cited by Defendant. In each instance, the party purporting to revoke his or her consent had knowledge that another individual had legitimate access to the system at some earlier point in time yet there was continued access to the network, computer or e-mail account after the relationship had lapsed. In this case, Plaintiff never authorized the forwarding of her e-mail let alone knew that it was occurring..

While the courts in the cases cited by Defendant sided with the interloper, the Second Circuit has imposed criminal liability under the Computer Fraud and Abuse Act when an individual exceeds earlier granted authorization.[39] As noted by Professor Kerr, other cases have established civil and criminal liability when an authorized user of a computer system exceeds the scope of his authorization.[40]

Defendant is correct that there was no implied withdrawal of consent. Consent to forward Plaintiff's e-mail was never given.

C. Inter-spousal immunity does not apply.

In *Anonymous v. Anonymous* and *Citron v. Citron*, the Second Circuit adopted the position that exceptions to the consent requirement of 18 U.S.C. § 2511(2)(d) may be implied in certain limited circumstances.[41,42] Over the past thirty-five years, this position has evolved into a minority view. The majority of circuits have consistently rejected an implied exception for

[38] Plaintiff's Statement of Undisputed Facts Nos. 24, 81-83.
[39] Morris, 928 F.2d 504
[40] Kerr, *Cybercrime's Scope: Intercepting "Access" and "Authorization" in Computer Misuse Statutes*, at 1632-37.
[41] *Anonymous v. Anonymous*, 558 F.2d 677 (2d. Cir. 1977).
[42] *Citron v. Citron*, 722 F.2d 14 (2d. Cir. 1983).

electronic surveillance between spouses.[43] *Anonymous* and *Citron* should be construed as being limited to their facts rather than establishing a blanket statutory exception to Wiretap Act liability during and after marriage.

Anonymous v. Anonymous involved allegations that an ex-husband tape recorded telephonic conversations between the ex-wife and the parties' minor child who resided with the ex-husband. The court recognized that the ex-husband tape recorded a conversation that he would have had the ability and right to listen in on pursuant to the extension phone exemption. contained within the statute. Notably, the court acknowledged that its decision was limited to the facts presented, "nor do we suggest that a plaintiff could never recover damages from his or her spouse under the federal wiretap statute."[44]

Citron v. Citron centered upon the narrow issue of whether the defendant, the former wife, acted willfully when she tape recorded telephone calls between her children and their father. The case does not stand for the proposition that inter-spousal immunity existed with respect to violations of the Wiretap Act, if even between former spouses, but simply that the statute required evidence of willful behavior.[45] As the statute was amended in 1986 to require evidence of intention, reliance upon *Citron* is questionable.

Defendant has also cited *Janecka v. Franklin* for the proposition that the law in the Second Circuit supports unrestricted spousal eavesdropping.[46] *Janecka*, like *Anonymous*, involved the father's recording of telephone conversations between a minor child and the child's mother. The recorder was based in the father's home. Notwithstanding the court's statements

---

[43] *See* Shana K. Rahavy, *The Federal Wiretapping Act: the Permissible Scope of Eavesdropping in the Family Home*, 2 J. High Tech. L.87, 91 (2003).
[44] *Anonymous*, 558 F.2d at 678-79.
[45] *Citron*, 722 F.2d at 15-16.
[46] *Janecka v. Franklin*, 684 F. Supp. 24 (S.D.N.Y. 1987), *aff'd* , 843 F.2d 110 (2d Cir. 1988).

regarding the use of federal courts in state child custody litigation, nothing in *Janecka,* alters the view that the case was properly decided under the parental consent exception. What distinguishes *Anonymous* and *Janecka* from the instant case, however, is the fact that virtually all of the intercepted e-mail does not directly involve children and that the "set it and forget nature" of e-mail auto-forwarding does not require any input or monitoring from the interloper.

Nothing contained within the Wiretap Act creates an explicit exception for spouses, ex-spouses or family members. The consent exception contained within 18 U.S.C. § 2511 permits the interception of an electronic communication where such person is a party to the communication or has given prior consent. Absent such consent, the only entity that may authorize an interception is a court of competent jurisdiction. Court's relying on the one-party consent exception in the context of parent-child monitoring do so on the basis that the parent has vicariously consented to the interception.[47]

The justification for wiretapping in the parent-child relationship - to protect the child - is simply not present in the spousal relationship. Further, the motivation for inter-spousal wiretapping is rarely benign but is usually calculated to gather evidence for purposes of divorce litigation.[48] And this is precisely what happened during the parties' marriage and after their separation and divorce.

The Second Circuit has not created a bar to inter-spousal liability for Wiretap Act violations. This court should not read such an exception into the statute.

---

[47] Rahavy, *supra,* at 89-90.

[48] *Kratz v. Kratz*, 477 F.Supp. 463, 476 (E.D. Pa. 1979) (Title III prohibits one method of obtaining evidence and "there is no more reason to permit husbands and wives to perpetrate these evils upon each other with impunity than there is to permit them legally to commit other crimes against each other.")

D. A fiduciary relationship existed between Plaintiff and Abadir when the MSA was signed.

Under New York law, the relationship between husband and wife is a fiduciary one "requiring the utmost of good faith" in dealings between them.[49] "When a fiduciary, in furtherance of [his] own individual interests, deals with the beneficiary of the duty in the matter relating to the fiduciary relationship, the fiduciary is strictly obligated to make full disclosure of all material facts."[50]

Agreements between spouses, unlike ordinary business contracts, involve a fiduciary relationship requiring the utmost of good faith. There is a strict surveillance of all transactions between married persons, especially separation agreements.[51]

In order to establish a cause of action for breach of a fiduciary duty with respect to the execution of the agreement, plaintiff must establish the existence of a fiduciary relationship, misconduct by defendant, and that such misconduct "induced plaintiff to engage in the transaction in question," directly causing the loss about which plaintiff complains.[52] Nondisclosure only becomes actionable, however, where a defendant has a duty to disclose, which can arise where there is a confidential or fiduciary relationship between the parties.[53]

In this instance, a fiduciary relationship existed between the parties at the time the MSA was executed by virtue of their marital relationship. During the period leading up to the execution of the MSA, Defendant Abadir never disclosed to Plaintiff that he was receiving her

---

[49] *von Bulow v. von Bulow*, 634 F. Supp. 1284, 1302 (S.D.N.Y. 1986) (citing *Christian v. Christian*, 42 N.Y.2d 63, 72, 365 N.E.2d 849, 855, 396 N.Y.S.2d 817, 823, (1977))("Defendant had a duty to disclose facts material to his wife's financial decisions concerning him. And there can be no doubt that the existence of a murder scheme would have been material to Mrs. von Bulow's actions in giving Mr. von Bulow an interest in her 1979 will and 1980 trust and, once given, preserving them.")

[50] *Harding v. Naseman*, 2008 U.S. Dist. LEXIS 92813 (S.D.N.Y., Nov. 13, 2008).

[51] *Christian v. Christian*, 42 N.Y.2d 63; 365 N.E.2d 849 (1977).

[52] *Laub v Faessel*, 297 A.D.2d 28, 31, 745 N.Y.S.2d 534 (2002).

[53] *Barron Partners, L.P. v. LAB123*, 2008 U.S. Dist. LEXIS 106813 (S.D. N.Y. 2008).

in-bound e-mail messages.[54] The MSA purports to contain a general release of liability, which if upheld, would result in Plaintiff's loss of her pre-MSA Wiretap Act claims which at a minimum would be $10,000, or $100 per day.

On the basis of this analysis, as a matter of law and fact, summary judgment should not enter as to Plaintiff's claim for breach of fiduciary duty.

E. Plaintiff is entitled to injunctive relief.

18 U.S.C. § 2520(b) permits a party to seek appropriate relief, including "preliminary and other equitable or declaratory relief as may be appropriate."

The act of an interception has been acknowledged by Defendant. While he claims that Plaintiff consented to the interception and that such consent was never revoked, he can no longer make such a claim. The filing and service of the lawsuit in December 2010 provided Defendant with such notice that Plaintiff does not consent to the disclosure or use of her e-mail.[55]

Each act of use and/or disclosure of an intercepted electronic communication constitutes a new violation, with a new two year statute of limitations and with new damages. However, the only means by which the material contained in the e-mail communications intercepted by Defendant can remain secure is to prevent Defendant from using or disclosing said material.

The undisputed facts and the applicable legal standards establish an entitlement to an injunction as a basis for relief. Accordingly, summary judgment with respect to Plaintiff's claim is not appropriate.

---

[54] Plaintiff's Statement of Undisputed Facts Nos. 27-29.

[55] *Register.com, Inc. v. Verio, Inc.*, 126 F.Supp. 2d 238, 249 (S.D.N.Y. 2000).

III. Conclusion

Defendant Abadir's motion for summary judgment should be denied in all respects. Critically, issues of fact exist with respect to whether Plaintiff consented to the interception of her e-mail and when she knew that that an interception was occurring. Whether the auto-forwarding of e-mail constitutes an interception is a matter over which there is no factual dispute.

Plaintiff's motion for partial summary should be granted with regard to auto-forwarding of e-mail as an interception under 18 U.S.C. § 2510; that a fiduciary relationship existed on the date that the MSA was executed, December 19, 2006; and that Defendant exceeded the consent which he claims Plaintiff granted by receiving e-mail messages not pertaining to the children.

Dated at Greenwich this 31st day of December 2013.

Respectfully submitted,

ANNABELLE ZARATZIAN

By 

Harold R. Burke (HB0149)
Law Offices of Harold R. Burke
21 Sherwood Place
Greenwich, CT 06830
Telephone: (203) 219-2301
Facsimile: (203) 413-4443
E-Mail: hrb@burke-legal.com

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANNABELLE ZARATZIAN PLAINTIFF	)	
V.	)	10 CIV 09049 (VB)
ADEL RAMSEY ABADIR AND LARRY M. CARLIN DEFENDANTS	)	

CERTIFICATION OF SERVICE

I hereby certify that on December 31, 2013 the foregoing motion was filed electronically and served electronically and by mail upon the following non-appearing counsel and pro se parties:

Nathaniel Z. Marmur, Esq.
BALLARD SPAHR STILLMAN &
FRIEDMAN LLP
425 Park Avenue
26th Floor
New York, NY 10022
nmarmur@stillmanfriedman.com

Larry M. Carlin, Esq.
437 Madison Avenue, Floor 35
New York, NY
lmcarlinlaw@msn.com

Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF System.

/s/ *Harold R. Burke*
Harold R. Burke (hb0149)
Law Offices of Harold R. Burke
P.O. Box 4078
21 Sherwood Place
Greenwich, CT 06830
Telephone: (203) 219-2301
Facsimile: (203) 413-4443
E-Mail: hrb@burke-legal.com